



- (51) International Patent Classification:
H04L 29/06 (2006.01)
- (21) International Application Number:
PCT/EP2012/056977
- (22) International Filing Date:
17 April 2012 (17.04.2012)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
1550/DEL/2011 31 May 2011 (31.05.2011) IN
- (71) Applicant (for all designated States except US): **ALCATEL LUCENT** [FR/FR]; 3 avenue Octave Gréard, F-75007 Paris (FR).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): **POTE, Parag Narayanrao** [IN/IN]; Alcatel-Lucent India Limited, Nagawara Village, Kasaba Taluk, Outer Ring Road, Manyata Embassy Business Pk, Bangalore 560045 (IN).
- (74) Agent: **MOUNEY, Jérôme**; 32 avenue Kléber, F-92700 Colombes (FR).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: DISTRIBUTED ACCESS CONTROL ACROSS THE NETWORK FIREWALLS

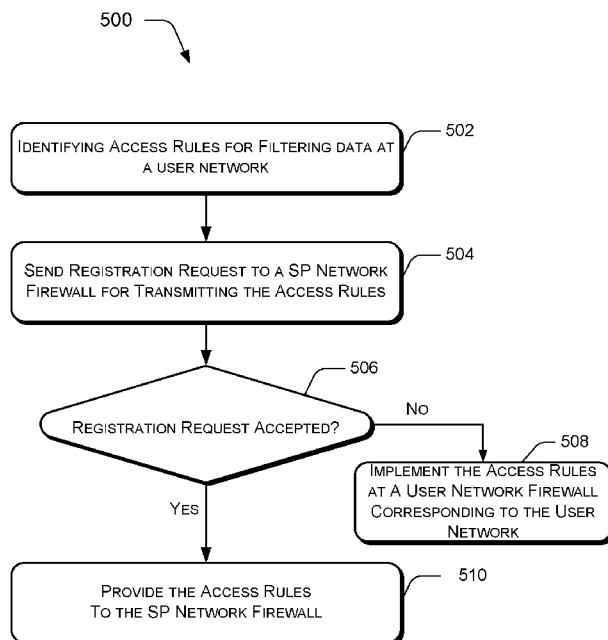


Fig. 5

(57) Abstract: The present subject matter discloses a method and a system for distributing access control across network firewalls. In one implementation, at least one access rule that can be implemented at a service provider network firewall (114) for filtering data directed to the user network (104) is identified at a user network (104). The at least one access rule is then provided to the service provider network firewall (114) for implementing the at least one access rule at a service provider network (106) corresponding to the service provider network firewall (114).



Published:

— *with international search report (Art. 21(3))*

DISTRIBUTED ACCESS CONTROL ACROSS THE NETWORK FIREWALLS

FIELD OF INVENTION

[0001] The present subject matter relates to network firewalls and, particularly but not exclusively, to distributed access control across the network firewalls.

BACKGROUND

[0002] Recent enhancements in computing and communication capabilities of various computing systems have made it easy for the computing systems to interact with each other over various communication networks. Further, the World Wide Web has enabled the computing systems to interact with each other across the globe. Such wide-spread reach and easy exchange of data has led to security concerns and privacy issues. In order to protect the computing systems from receiving or sending unauthorized content, variety of protection techniques has been implemented.

[0003] One such protection technique includes deploying firewalls. The firewalls are typically configured to regulate what content is allowed into and out of a computing system or a network. The firewall may be installed in many different places on the network, for example, at an entry or exit point in the network, i.e., on a dedicated computing system, such as a router through which the network, such as a user network connects to another network, such as a service provider network. Additionally, the firewall may be installed on an individual computing system to regulate communication for that computing system.

[0004] Generally, the firewalls are configured to permit authorized content and block unauthorized content from entering and leaving the network based on various access rules, for example, IP (Internet protocol) address-based rules, content-based rules, and application-based rules. However, such monitoring and regulation of the unauthorized content may consume a considerable amount of resources, for example, bandwidth of the network, and may adversely affect the performance of the network. For instance, data received at the user network typically includes the unauthorized content as well as the authorized content. The unauthorized content may consume a large part of bandwidth available for the network connection, thus affecting network speed and the overall performance of the user network.

SUMMARY

[0005] This summary is provided to introduce concepts related to distribution of access control across network firewalls. This summary is not intended to identify essential features of the claimed subject matter nor is it directed to use in determining or limiting the scope of the claimed subject matter.

[0006] In an embodiment, a method includes identifying access rules at a user network. The access rules are implementable at a service provider network firewall for filtering data directed to the user network. Further, the access rules are provided to the service provider network firewall for filtering the data directed to the user network. In one implementation, the access rules are provided using a distributed access control protocol.

[0007] In another embodiment, a method includes receiving access rules from a user network. The access rules are implemented at the service provider network firewall for filtering the data directed to the user network. In one implementation, the access rules are received using a distributed access control protocol.

[0008] In yet another embodiment, a user network access control (UNAC) system is described. The UNAC system includes a processor and a memory coupled to the processor. The memory includes a user network access rule configuration (UNARC) module configured to identify access rules implementable at a service provider network firewall for filtering data directed to a user network. The UNAC system further includes a user network interaction module configured to provide the access rules to the service provider network firewall.

[0009] In accordance with another embodiment, a service provider access control (SPAC) system is described. The SPAC system includes a processor and a memory coupled to the processor. The memory includes a service provider interaction module configured to receive access rules. The SPAC system further includes a service provider network access control module configured to filter unauthorized data from data directed to a user network based on the access rules.

[0010] In accordance with yet another embodiment of the present subject matter, a computer readable medium having embodied thereon a computer program for executing a method is described. The computer readable medium perform acts including identifying an

access rule at a user network. The access rule is implementable at a service provider network firewall for filtering data directed to the user network. Further, access rule may be provided to the service provider network firewall for implementing the access rule at a service provider network corresponding to the service provider network firewall.

[0011] In accordance with another embodiment of the present subject matter, a computer readable medium having embodied thereon a computer program for executing a method is described. The computer readable medium perform acts including receiving an access rule from a user network firewall. Further, the access rule is implemented at a service provider network firewall for filtering data directed towards a user network corresponding to the user network firewall.

BRIEF DESCRIPTION OF THE FIGURES

[0012] The detailed description is described with reference to the accompanying figures. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The same numbers are used throughout the figures to reference like features and components. Some embodiments of system and/or methods in accordance with embodiments of the present subject matter are now described, by way of example only, and with reference to the accompanying figures, in which:

[0013] Figure 1 illustrates an exemplary network implementation of access control distribution across network firewalls, according to an embodiment of the present invention;

[0014] Figure 2 illustrates exemplary components of a user network access control system in communication with a service provider access control system, in accordance with an embodiment of the present subject matter;

[0015] Figures 3a, 3b, 3c, and 3d show exemplary packet formats for a distributed access control protocol for implementing access control distribution across the network firewalls, according to an embodiment of the present subject matter;

[0016] Figure 4 illustrates communication across network firewalls for implementing access control distribution across the network firewalls, in accordance with an embodiment of the present subject matter;

[0017] Figure 5 illustrates a method for distributing access rules by a user network firewall, in accordance with an embodiment of the present subject matter; and

[0018] Figure 6 illustrates a method for configuring a service provider network firewall to implement access control, according to an embodiment of the present subject matter.

[0019] It should be appreciated by those skilled in the art that any block diagrams herein represent conceptual views of illustrative systems embodying the principles of the present subject matter. Similarly, it will be appreciated that any flow charts, flow diagrams, state transition diagrams, pseudo code, and the like represent various processes which may be substantially represented in computer readable medium and so executed by a computer or processor, whether or not such computer or processor is explicitly shown.

DESCRIPTION OF EMBODIMENTS

[0020] The present subject matter relates to methods and systems for providing access control at, at least, one service provider (SP) network firewall. The network firewalls may be hardware device, software program running on a secure host computing system, or a combination thereof.

[0021] A firewall is typically deployed in a network to permit authorized data and block unauthorized data from entering and leaving the network. The authorized data may be understood as the data identified by a network administrator as being necessary and safe for the network, for instance, data from a client site, data having only text document, and data from one or more recognized IP addresses. The unauthorized data may be understood as the data identified by a network administrator as being unnecessary and harmful for the network, for instance, data from a social networking site, spam mails, data having audio or video content, and data from one or more IP addresses recognized as being unsafe for the network. Based on certain parameters, data may be allowed to pass through the firewall to its destination or may be blocked by the firewall. These parameters may be based on a variety of data characteristics and are regulated based on access rules, for example, IP address based rules, content based rules, and application based rules. The access rules may be defined, for example, by a network administrator.

[0022] The IP address based rules may include rules for blocking data coming from or going to any particular IP addresses or website. For example, data coming from or going to any

particular website may be blocked based on, say, IP address, and Media Access Control (MAC) address. The content based rules may include rules for blocking any data based on the content of the data. For example, the firewall may be configured to block data having content, such as audio files, video files, and executable files or content having one or more specified words, such as mail, job, music, and movie. The application based rules may include rules for blocking data coming from or going to any particular type of website. For example, data coming from or going to job portals, social networking websites, blogs, music download websites, and e-mail access websites.

[0023] Firewalls are usually deployed at an edge, i.e., an entry/exit point in a network so that the data transmitted between one network and another network can be monitored and accordingly, entry and exit of the data can be controlled. For example, a firewall may be deployed in a user network to monitor data received from a service provider (SP) network, which is connected to a public network. The user network may be understood as a network used or operated by an entity, such as an enterprise, a company, an institution or an individual for enabling internet access for user devices, such as computing devices connected to the user network. The user network may deploy the firewall to filter data coming from the SP network. For example, the user network set up by an enterprise may be configured to block data pertaining to job portals or social networking sites or adult sites or porn sites. Similarly, the user network set up by individuals in a residential complex may be configured to block data having content inappropriate for children or data associated with gaming sites.

[0024] The SP network may be understood as a network implemented by a service provider which provides access to public network, such as the Internet, ISDN, PSTN, and other content services. The entity thus receives and transmits data from public network, such as the Internet, using the SP network. The SP network typically accesses the Internet via a high speed trunk network, such as a fiber optic network, and provides the access to the Internet to the user network via network connections of smaller bandwidth. The SP network may deploy the firewall to monitor data coming from the public network, or the Internet and block malicious data from being transmitted to or from the user network. However, the SP network typically permits all or most data traffic into the user network, leaving it to the user network to block the unauthorized data using the firewalls. Transmitting all the data to the user network consumes a considerable amount of resources, for example, access bandwidth from the SP network to the user network,

and may adversely affect the performance of the user network. For example, the user network may have a network connection of 100 Mbps bandwidth for exchanging data with the SP network. Now, if at some point of time the SP network receives 100 megabytes (Mb) of data from the Internet and transmits the data to the user network, the bandwidth of the user network would be fully consumed for around one second. However, if out of the 100 Mb data, 30 Mb of data include content that is unauthorized according to the access rules applied at the user network firewall, the user network firewall will block the 30 Mb of data from entering the user network. For example, malicious entities may attempt to flood the user network by regularly transmitting unauthorized data. Thus, 30% bandwidth of the network connection could be said to be unutilized for the user network, thus affecting performance of the network. Thus, while the cost is paid for the entire bandwidth of the network connection, the complete bandwidth remains underutilized resulting in additional costs.

[0025] Additionally, in case of large networks and upgraded network topologies, the number of access rules is large to accommodate for various threats to the performance of the network and data security. With increasing complexity of network topologies and stringent requirements for access control, configuring rules in a firewall has become difficult.

[0026] According to an embodiment of the present subject matter, systems and methods for distributing access control across network firewalls, for example, across the user network firewall, deployed at user network, and at least one SP network firewall, deployed at SP network corresponding to the user network, are described. In one embodiment, to implement access control distribution across such networks, one or more access rules are identified and transmitted to the SP network firewall. The one or more access rules include access rules that can be deployed at the SP network firewall to regulate user network access at the service provider's end. The SP network may use the access rules to filter data entering or leaving the user network, thus reducing load on the user network firewall. Sharing the access rules with the SP network firewall also results in proper utilization of user network's bandwidth. Additionally, filtering data at the service provider's end may also provide an additional layer of safety for the user network. Further, the number of access rules shared between the user network and the SP network may vary based factors, such as requirements of the user network or a contract between the user network and the SP network. For example, in one scenario the user network may transmit only

few access rules to the SP network, in another scenario, the user network may transmit substantially all the access rules to the SP network.

[0027] In one implementation, the distribution of access control is initiated at the user network firewall, for example, during booting of the user network firewall. The user network firewall is configured to transfer the access rules to the SP network firewall. For example, the access rules may include Internet protocol (IP) addresses, port addresses, and access control content, based on which the incoming data may be blocked at the SP network firewall. In one implementation, the user network firewall may initially send a registration request to the SP network firewall. On acceptance of the registration request, i.e., upon successful authentication of the user network firewall, the user network firewall sends the access rules to the SP network firewall.

[0028] Upon receipt of the access rules from the user network firewall, the SP network firewall applies the received access rules for the authorized user network. For example, the SP network firewall may add the received access rules to the access rules already existing at the SP network firewall's end. Alternatively, the SP network firewall may create a new set of access rules based on the access rules received from the user network firewall. Further, the user network firewall may also prompt updates in previously transferred access rules to the SP network firewall. For example, the user network firewall may provide a few more IP addresses to update an existing list of IP addresses according to which data pertaining to a job portal is to be blocked. Based on the updated or new set of access rules, the SP network firewall blocks all the unauthorized data at the SP network, thus reducing data traffic on the user network.

[0029] In one implementation, the access rules may be exchanged between the user network firewall and the SP network firewall using a data transmission protocol, for instance, a distributed access control protocol (DACP). In an implementation, a DACP header may be configured and appended with a header of the data packets exchanged as a part of transfer of the access rules to the SP network firewall. The DACP header may include, for example, an authentication key, source IP address, command types, and version of the DACP used for transmission of the data packets.

[0030] Distribution of access rules between the user network firewall and the SP network firewall, thus introduces an advanced level of data filtering at the SP network firewall, as the data

entering the user network is now filtered at the SP network firewall. Additionally, data may also be filtered at the user network firewall based on any access rule that has not been shared with the SP network firewall. Further, as the unauthorized data directed to the user network is blocked at the SP network, the resources, such as bandwidth at the user network are optimally utilized. Also, the SP network firewall is generally a high performance firewall having advanced capabilities. Thus, the distribution of the access rules allows the user network firewall to utilize the capabilities of the high performance SP network firewall. Hence, a low performance low cost variant of a firewall can be deployed as the user network firewall in the user network. In one implementation, the SP network firewall may be provided for filtering the unauthorized data directed to the user network, as an additional service by charging fees such as registration fees.

[0031] Although the present subject matter has been described in relation to communication between two networks, such as a user network and a SP network, it will be understood that the access rules distribution may also be used in multiple level networks, such that a lower level network shares its access rules with a higher level network.

[0032] It should be noted that the description and figures merely illustrate the principles of the present subject matter. It will thus be appreciated that those skilled in the art will be able to devise various arrangements that, although not explicitly described or shown herein, embody the principles of the present subject matter and are included within its spirit and scope. Furthermore, all examples recited herein are principally intended expressly to be only for pedagogical purposes to aid the reader in understanding the principles of the present subject matter and the concepts contributed by the inventor(s) to furthering the art, and are to be construed as being without limitation to such specifically recited examples and conditions. Moreover, all statements herein reciting principles, aspects, and embodiments of the present subject matter, as well as specific examples thereof, are intended to encompass equivalents thereof.

[0033] It will also be appreciated by those skilled in the art that the words during, while, and when as used herein are not exact terms that mean an action takes place instantly upon an initiating action but that there may be some small but reasonable delay, such as a propagation delay, between the initial action and the reaction that is initiated by the initial action.

[0034] Fig. 1 illustrates an exemplary network environment 100 for implementing access control distribution across network firewalls, according to an embodiment of the present subject

matter. The network 100 includes one or more user devices 102-1, 102-2,..., 102-n, hereinafter referred to as the user device(s) 102, connected to a user network 104. The user network 104 may be a wireless network, wired network or a combination thereof. The user network 104 can be implemented as one of the different types of networks, such as intranet, local area network (LAN), wide area network (WAN), the Internet. The user network 104 may either be a dedicated network or a shared network, which represents an association of the different types of networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), Transmission Control Protocol/Internet Protocol (TCP/IP), and Wireless Application Protocol (WAP), to communicate with each other. In one embodiment, the user network 104 may be understood as an enterprise network operated by an entity, such as a company or an institution for providing internet access to user devices 102 connected to the user network 104. In another embodiment, the user network 104 may be a network operated by, say, one or more individuals living in a residential complex.

[0035] The user devices 102 include, but are not limited to, computing devices such as mainframe computers, workstations, personal computers, desktop computers, minicomputers, servers, multiprocessor systems, and laptops; cellular communication devices such as a personal digital assistants, smart phones, mobile phones; and the like. The user devices 102 connect to the user network 104 to access or receive data from the Internet or other computing systems connected to the Internet. For the purpose, the user network 104 is connected to a service provider (SP) network 106. The SP network 106 is in turn connected to an Internet cloud (not shown in Figure), such as the World Wide Web. The SP network 106 may be defined as a network set up by a service provider for providing internet access to the user network 104. The SP network 106 typically connects to the Internet cloud, for accessing the Internet, via a high speed network, such as a fiber optic network. The SP network 106 in turn provides the user network 104 access to the Internet via transmission lines of smaller bandwidth, such as copper wires. The user network 104 thus receives and transmits data from the Internet using the SP network 106.

[0036] Thus, when the user devices 102 need to access the Internet, the user devices 102 connect to the user network 104. The user network 104 in turn connects to the SP network 106 to provide internet access to the user devices 102. The user devices 102 may thus send data, in the form of data packets, to any other computing device over the Internet through the user network

104 and the SP network 106. Similarly, when any other computing system needs to send any data to the user devices 102, the data is first received by the SP network 106 that routes the data to the user network 104 in the form of data packets. The user network 104 then routes the data packets to the user devices 102. However, before routing the data packets, the SP network 106 and the user network 104 scan the data packets to filter out and block unauthorized data and allow only authorized data to enter or leave the user network 104.

[0037] The unauthorized data may be understood as the data identified, for example, by a network administrator as being unnecessary and harmful for the network, for instance, data from a social networking site, data having audio or video content, any executable file, data from one or more IP addresses recognized as being harmful for the network, and the like. The authorized data may be understood as the data identified as being necessary and safe for the network, for instance, data from a client site, data having only text document, and data from one or more recognized IP addresses.

[0038] In one embodiment, each of the user network 104 and the SP network 106 includes one or more access control systems (not shown in Figure) having firewalls for regulating incoming and outgoing data to block the unauthorized data from entering or leaving the networks 104 and 106. For instance, the user network 104 includes a user network access control (UNAC) system 108 having a user network firewall 110 configured to prevent any unauthorized data from reaching the user devices 102. Similarly, the SP network 106 includes a service provider access control (SPAC) system 112 having a SP network firewall 114 configured to filter the unauthorized data across the SP network 106 to prevent any unauthorized data from reaching the user network 104. The access control systems 108, 112 may be, for example, a network device, such as a router or a gateway; a secure hosting computing system; or a network management server hosting the firewalls. Further, the firewalls 110, 114 may be implemented as stateful firewalls, stateful firewalls with application-level filters, stateless firewalls, network layer firewalls, application-proxy firewalls, and so on. However, it would be obvious that the present invention is not limited to use with any one specific type of firewall or access control system any can be extended to any type of firewall and access control system.

[0039] Each of the firewalls 110, 114 is configured to block the unauthorized data based on one or more access rules, for example, IP address based rules, content based rules, and

application based rules. The IP address based rules may include rules for blocking data coming from or going to any particular IP addresses or website. For example, data coming from or going to any particular website may be blocked based on, say, IP address, and Media Access Control (MAC) address. The content based rules may include rules for blocking any data based on content of the data. For example, the firewalls 110, 114 may be configured to block data having content, such as audio files, video files, and executable files or content having one or more specified words, such as mail, job, music, and movie. The application based rules may include rules for blocking data relating to any particular type of website. For example, data coming from or going to job portals, social networking websites, blogs, music download websites, and e-mail access websites. Further, the access rules may be defined, for example, by a system administrator.

[0040] In one implementation, the access rules are distributed across the SP network firewall 114 and the user network firewall 110 such that the SP network firewall 114 blocks some of the unauthorized data from entering the user network 104. For the purpose, one or more access rules are identified and transmitted by the user network firewall 110 to the SP network firewall 114. The one or more access rules include access rules that can be deployed at the SP network firewall 114 for regulating access to the user network 104 at the service provider's end.

[0041] In one implementation, the access rules for the user network firewall 110 are defined either as shared access rules or non-shared access rules. The shared access rules may be defined as the access rules that can be transferred and deployed at the SP network firewall 114 to block unauthorized data from entering or leaving the user network 104. In one implementation, the shared access rules may include rules to block data from untrustworthy sources. As mentioned previously, the SP network firewall 114 may generally be a high performance firewall with advanced capabilities. Accordingly, by distributing the shared access rules, the user network firewall 110 can utilize the capabilities of the high performance SP network firewall 114 to block sources that pose a high threat to the security of the user network 104. At the same time, access rules that are not very critical may be non-shared access rules that are configured locally using the user network firewall 110. In one embodiment, the shared access rules and the non-shared access rules may be selected based on firewall services subscribed by the user network 104. For instance, on subscribing a firewall services with low service charges, the user network firewall 110 may be allowed to provide only a limited number of access rules to the SP network firewall

for implementation at the SP network 106. The user network firewall 110 in such a case may provide only a few access rules to the SP network firewall 114.

[0042] For example, the shared access rules may include a list of IP addresses and port addresses from which the user network 104 will not accept incoming data. The non-shared access rules may include access rules that are deployed at the user network firewall 110 to block unauthorized data from accessing the user devices 102. For example, the non-shared access rules may include a list of IP addresses and port addresses according to which the incoming data may be blocked for the user devices 102 having the IP addresses and/or port addresses. Additionally, the non-shared access rules may include access rules that the network administrator does not want to share with the service provider in order to maintain secrecy, for example, the user network 104 may not want the service provider to know that data from a particular organization, say, a bank is not trusted and disallowed by the user network 104.

[0043] For distributing the access control across the network firewalls 110, 114, the user network firewall 110 includes a user network interaction module 116 configured to facilitate interaction, such as exchange of access rules between the user network firewall 110 and the SP network firewall 114. The user network interaction module 116, hereinafter referred to as the UNI module 116 is configured to transfer the access rules, in the form of data packets, to the SP network firewall 114. In one embodiment, the user network firewall 110 may use a data transmission protocol, for instance, a distributed access control protocol (DACP) for transmitting the access rules to the SP network firewall 114. The DACP may be implemented, for example, as a transmission control protocol (TCP) based protocol to regulate the exchange of the access rules and other information between the user network 104 and the SP network 106. In one implementation, a DACP header can be configured and appended with the header on the data packets, which are transmitted as a part of transfer of the shared access rules to the SP network firewall 114. The DACP header can include, for example, an authentication key, source IP address, command types, and version of the DACP used for transmission of the data packets. The DACP is further explained with reference to figure 3.

[0044] Further, the SP network firewall 114 includes a SP interaction module 118 similar to the UNI module 116. The SP interaction module 118 is configured to facilitate interaction, such as exchange of access rules between the user network firewall 110 and the SP network

firewall 114. On receiving the access rules, the SP network firewall 114 adds the access rules to already existing access rules configured with the SP network firewall 114. Additionally or alternatively, the SP network firewall 114 may create a new set of access rules based on the access rules received from the user network firewall 110. Based on the updated or new set of access rules, the SP network firewall 114 starts regulating the data packets entering the user network 104 and blocks all the unauthorized data at the SP network 106, thus reducing data traffic on the user network 104.

[0045] Blocking the unauthorized data at the SP network 106 prevents unwanted and harmful data from entering the user network 104, improving the bandwidth utilization and in turn the network performance at the user network's end. Further, distributing the access rules to the SP network firewall 114 helps in utilizing data filtering capacity of the SP network firewall 114 as SP network firewalls are typically advanced and high processing firewalls capable of regulating large amount of data in lesser time as compared to user network firewalls. Additionally or alternatively, blocking the unauthorized data for the user network 104 may be provided as a chargeable service thus benefiting a service provider of the SP network 106.

[0046] Figure 2 illustrates exemplary components of the UNAC system 108 and the SPAC system 112, in accordance with an embodiment of the present subject matter. Examples of the UNAC system 108 and the SPAC system 112 include, but are not limited to, network devices, such as routers or gateways; secure host computing devices, such as mainframe computers, workstations, personal computers, desktop computers, minicomputers, servers, multiprocessor systems, and laptops hosting firewalls.

[0047] The UNAC system 108 includes one or more UNAC processor(s) 202, UNAC I/O interface(s) 204, and an UNAC memory 206, whereas the SPAC system 112 includes one or more SPAC processor(s) 208, SPAC I/O interface(s) 210, and a SPAC memory 212. Each of the processors 202, 208 can be a single processing unit or a number of units, all of which could also include multiple computing units. Each of the processors 202, 208 may be implemented as one or more microprocessors, microcomputers, microcontrollers, digital signal processors, central processing units, state machines, logic circuitries, and/or any devices that manipulate signals based on operational instructions. Among other capabilities, the processors 202, 208 are

configured to fetch and execute computer-readable instructions and data stored in the memory 206, 212, respectively.

[0048] Functions of the various elements shown in the figures, including any functional blocks labeled as “processor(s)”, may be provided through the use of dedicated hardware as well as hardware capable of executing software in association with appropriate software. When provided by a processor, the functions may be provided by a single dedicated processor, by a single shared processor, or by a plurality of individual processors, some of which may be shared. Moreover, explicit use of the term “processor” should not be construed to refer exclusively to hardware capable of executing software, and may implicitly include, without limitation, digital signal processor (DSP) hardware, network processor, application specific integrated circuit (ASIC), field programmable gate array (FPGA), read only memory (ROM) for storing software, random access memory (RAM), and non volatile storage. Other hardware, conventional and/or custom, may also be included.

[0049] The I/O interfaces 204, 210 may include a variety of software and hardware interfaces, for example, interface for peripheral device(s), such as a keyboard, a mouse, an external memory, and a printer. Further, the I/O interfaces 204, 210 may enable the UNAC system 108 and the SPAC system 112 to communicate with other computing devices, such as a personal computer, a laptop, and the like.

[0050] The memory 206, 212 may include any computer-readable medium known in the art including, for example, volatile memory such as static random access memory (SRAM) and dynamic random access memory (DRAM), and/or non-volatile memory, such as read only memory (ROM), erasable programmable ROM, flash memories, hard disks, optical disks, and magnetic tapes.

[0051] In one implementation, the UNAC memory 206 includes UNAC module(s) 214 and UNAC data 216. The UNAC module(s) 214 include routines, programs, objects, components, data structures, etc., which perform particular tasks or implement particular abstract data types. The UNAC module(s) 214 further include the user network firewall 110, a user network access rule configuration (UNARC) module 218, and other UNAC module(s) 220. The other UNAC module(s) 220 may include programs or coded instructions that supplement applications and functions of the UNAC system 108.

[0052] On the other hand, the UNAC data 216, amongst other things, serves as a repository for storing data processed, received, and generated by one or more of the module(s) 214. The UNAC data 216 includes, for example, user network access rule data 222, and other UNAC data 224. The other UNAC data 224 includes data generated as a result of the execution of one or more modules in the other UNAC module(s) 220.

[0053] Further, the SPAC memory 212 includes SPAC module(s) 226 and SPAC data 228. The SPAC module(s) 226 include routines, programs, objects, components, data structures, etc., which perform particular tasks or implement particular abstract data types. The SPAC module(s) 226 further include the SP network firewall 114, a SP access rule configuration (SPARC) module 230, and other SPAC module(s) 232. The other SPAC module(s) 232 may include programs or coded instructions that supplement applications and functions of the SPAC system 112. Additionally, although the SPARC module 230 has been shown external to the SP network firewall 114, however, it will be understood that the SPARC module 230 may be integral to the SP network firewall 114.

[0054] On the other hand, the SPAC data 228, amongst other things, serves as a repository for storing data processed, received, and generated by one or more of the module(s) 226. The SPAC data 228 includes, for example, SP access rule data 234, and other SPAC data 236. The other SPAC data 236 includes data generated as a result of the execution of one or more modules in the other SPAC module(s) 232.

[0055] As described previously, the user network firewall 110 is configured to identify and provide one or more access rules to the SP network firewall 114 such that based on the one or more access rules the SP network firewall 114 blocks unauthorized data from entering the user network 104. For the purpose, the UNARC module 218 may be configured to access an access rules list and identify the access rules that can be shared with the SP network firewall 114. In one implementation, the access rules may be identified and selected based on inputs received from a network administrator. The access rules may then be saved in the user network access rule data 222. Although the UNARC module 218 has been shown external to the user network firewall 110, however, it will be understood that the UNARC module 218 may be integral to the user network firewall 110.

[0056] In one implementation, the access rules may be defined either as the shared access rules or the non-shared access rules such that based on the shared access rules the SP network firewall 114 blocks unauthorized data from entering the user network 104. For the purpose, the UNARC module 218 is configured to access the user network access rule data 222 and define the access rules as shared access rules that can be transmitted to the SP network firewall 114 for blocking the unauthorized data from entering the user network 104. The UNARC module 218 may then save the shared access rules in shared access rules data 238 provided in the user network access rule data 222. In one implementation, the shared access rules data 238 may be used for implementing the shared access rules at the user network firewall 110 when the SP network firewall 114 is unable to perform the required filtering. Further, the remaining access rules may be defined as the non-shared access rules and saved in non-shared access rules data 240 provided in the user network access rule data 222.

[0057] Once defined, the shared access rules may then be distributed by the user network firewall 110 to the SP network firewall 114, for example, during booting of the user network firewall 110. For instance, each time the user network firewall 110 is booted, the UNI module 116 may obtain a list of the shared access rules from the shared access rules data 238 and provide the shared access rules to the SP network firewall 114. The shared access rules may be communicated to the SP network firewall 114 through various techniques. As previously described, the shared access rules may be transmitted using a data transmission protocol, for instance, the DACP. The DACP is further explained with reference to figure 3. In various other embodiments, the access rules may be provided using other transmission mediums such as emails or portable storage device.

[0058] The UNI module 116 initially establishes a connection with the SP interaction module 118, for example, by using a handshake mechanism. The UNI module 116 may then send a registration request to the SP interaction module 118 to seek permission for transferring the shared access rules to the SP network firewall 114. The SP interaction module 118 may then allow or reject the registration request from the UNI module 116 and send a registration reply to the UNI module 116. If the registration request is accepted, the UNI module 116 may send the shared access rules, for example, in the form of data packets. Further, the UNI module 116 may also transmit an authentication key, such as a hash value, along with or before the shared access rules, to enable authenticated exchange of data between the user network firewall 110 and the SP

network firewall 114. Additionally or alternatively, the shared access rules may be encrypted at the user network firewall 110, say, by the UNI module 116 before such access rules are provided to the SP network firewall 114. The encryption ensures secure transmission of the shared access rules.

[0059] The SP interaction module 118, on receiving the shared access rules, decrypts the shared access rules and adds them to the already existing access rules saved in the SP access rules data 234. In one implementation, the SP access rules data 234 includes one or more access rules data 242-1, 242-2, 242-3, ..., 242-n, hereinafter referred to as the access rules data 242, for saving access rules corresponding to one or more user networks connected to the SP network 106. For example, the access rules data 242-1 may be provided to save the access rules corresponding to the user network 104. Additionally or alternatively, the SP network firewall 114 may also create a new set of SP access rules data 234 based on the access rules received from the user network firewall 110. The access rules data 242 may then be used by the SP network firewall 114 to regulate data traffic entering or leaving the user network 104, for example, by blocking the unauthorized data entering the user network 104.

[0060] In operation, when some data packets directed towards the user device 102 are received by the SP network 106 through the Internet cloud, the data packets are analyzed by the SP network firewall 114 to ascertain whether the data packets contain any unauthorized data. For the purpose, the SPARC module 230 accesses the access rules data 242 to obtain the shared access rules for the user network 104. The shared access rules may then be provided to a SP access control module 244 of the SP network firewall 114 for filtering unauthorized data from the data packets. The SP access control module 244 then analyzes the data packets and identifies the unauthorized data based on the shared access rules. For example, if the data packets include data from a social networking website and the shared access rules contain a rule for blocking data from social networking websites then the SP access control module 244 identifies the data as unauthorized data. The unauthorized data is then filtered out from the data packets and filtered data packets are routed to the user network 104.

[0061] The filtered data packets are received by the user network 104 and routed to the user network firewall 110. The user network firewall 110 analyzes the filtered data packets to ascertain whether the data packets contain any unauthorized data. For the purpose, the UNARC

module 218 accesses the non-shared access rules data 240 to obtain the non-shared access rules for the user network 104. The non-shared access rules may be provided to a user network access control module 246, provided in the user network firewall 110, for filtering unauthorized data from the filtered data packets. The user network access control module 246 analyzes the filtered data packets and identifies the unauthorized data based on the non-shared access rules. For example, if the data packets include data from a particular banking site and the non-shared access rules contain a rule for blocking data from the particular banking site then the user network access control module 246 identifies the data as unauthorized data. The unauthorized data is filtered out from the filtered data packets and re-filtered data packets are routed to the user devices 102.

[0062] Figures 3a, 3b, 3c, and 3d show exemplary packet formats for sending shared access rules according to the DACP for implementing access control distribution across the user network firewall 110 and the SP network firewall 114, according to an embodiment of the present subject matter. As described previously, the user network firewall 110 and the SP network firewall 114 use the DACP for transmitting the shared access rules to the SP network firewall 114. For the purpose of explanation, and not as a limitation, the DACP is implemented as a transmission control protocol (TCP) based protocol. It would be obvious to a person skilled in the art that the DACP may also be implemented as other data transmission protocols, such as user datagram protocol.

[0063] Figure 3a illustrates a data packet 300 with the shared access rules appended according to the DACP. The data packet 300 includes an IP header 302 having the IP address of the computing device to which the data packet is to be transmitted; a TCP header 304, and a DACP header 306 having data, such as commands and shared access rules from a source network firewall, sending the data packet 300, for a destination network firewall.

[0064] Figure 3b illustrates packet formats for the DACP header 306, according to an embodiment. In one implementation, the DACP header 306 includes three parameters: a first parameter referred to as commands 308, a second parameter referred to as versions 310, and a third parameter referred to as a reserve 312. The commands 308 include commands from the source network firewall, say, the user network firewall 110 for the destination network firewall, say, the SP network firewall 114. Examples of the commands 308 include, but are not limited to,

command for registration, and command for updating the access rules. The command for registration may be defined as registration request sent by the user network firewall 110 to the SP network firewall 114 to seek permission for transferring the shared access rules to the SP network firewall 114. The command for updating access rules may be defined as the command sent by the user network firewall 110 to the SP network firewall 114 for updating the shared access rules for the user network 104.

[0065] Figure 3c illustrates packet formats for the DACP header 306 when the command for registration is included in the commands 308. The command for registration is hereinafter referred to as a registration command 314. The DACP header 306, in such a case, includes the registration command 314, the versions 310, the reserved 312, a source IP address 316, an authentication key 318, keep-alive intervals 320, and number of keep alive intervals 322. The registration command 314, as previously described, includes a registration request from the user network firewall 110 seeking permission for transferring the shared access rules to the SP network firewall 114. The source IP address 316 includes IP address of the network firewall sending the data packet 300, i.e., the user network firewall 110. The authentication key 318 includes, for example, a hash value for enabling authorized exchange of data between the user network 104 and the SP network 106. The authentication key 318 may be used by the SP network firewall 114 to authenticate the shared access rules sent by the user network firewall 110. Further, the hash value may be generated using pre-existing parameters available with the user network 104 and the service provider network 106. For example, the hash value may be generated using the source IP address and a pre-shared key using any known hashing algorithm. Additionally or alternatively, the authentication key may be an encrypted key. The keep-alive intervals 320 include handshake data sent by the source network firewall for verifying whether the destination firewall is active and ready for filtering data. The handshake data may include, for example, the time intervals at which the user network firewall 110 and the SP network firewall 114 need to perform a keep-alive check. The number of keep alive intervals 322 includes data related to number of times the keep-alive check is performed before declaring the connection broken.

[0066] Figure 3d illustrates packet formats for the DACP header 306 when the command sent in the commands 308 is the command for updating access rules. The command for updating access rules is hereinafter referred to as an update command 324. The DACP header 306, in such

a case, includes the update command 324, the versions 310, the reserved 312, the source IP address 316, and the authentication key 318. In addition, the DACP header 306 also includes total number of entries 326, and one or more update blocks 328. The update command 324, as previously described, pertains to a command sent by the user network firewall 110 to the SP network firewall 114 for either updating the shared access rules or creating new access rules for the user network 104. Based on the update command 324 the SP network firewall 114 updates the access rules data 242 corresponding to the user network 104. The total number of entries 326 may include the total number of shared access rules sent by the user network firewall 110 in the present data packet, i.e., the data packet 300. Providing the total number of entries 326 helps the SP network firewall 114 to estimate the total number of shared access rules being sent in the data packet 300. The update block 328 includes data related to the shared access rules transmitted by the user network firewall 110 along with the data packet 300. For example, the update block 328 includes data related to a first shared access rule sent in the data packet 300.

[0067] In one implementation, the update block 328 includes an entry number 330, an IP protocol 332, a source IP address 334, a destination IP address 336, a source port 338, and a destination port 340. The entry number 330 corresponds to the entry number of the shared access rule in the list of shared access rules sent with the data packet 300. For example, entry number 330 for the update header 328-1 would be 1, similarly entry number 330 for the update header 328-n would be 'n'. The source IP address 334 includes IP address from which incoming data is to be filtered by the SP network firewall 114. The destination IP address 336 includes IP address of the destination computing device, for instance, destination address 336 would include IP address of the user devices 102 for which the data coming from the source IP address 334 is to be blocked. The source port 338 includes port address of computing devices corresponding to the source IP address 334 from which the incoming data is to be blocked. The destination port 340 includes destination port address of the user devices 102 for which the data coming from the source IP address 334 is to be blocked.

[0068] Figure 4 illustrates communication between the user network firewall 110 and the SP network firewall 114 for implementing access control distribution across the network firewalls 110 and 114, in accordance with an embodiment of the present subject matter. According to the embodiment depicted in the figure, the user network firewall 110 communicates with the SP network firewall 114 using the DACP.

[0069] The user network firewall 110 initially establishes a connection with the SP network firewall 114 by using a handshake mechanism. For instance, the UNI module 116 of the user network firewall 110 sends a TCP synchronization command 402, to the SP interaction module 118 of the SP network firewall 114 for establishing connection between both the network firewalls 110 and 114. The synchronization command may include, for example, details such as IP address of the user network firewall 110. The SP network firewall 114 replies to the TCP synchronization command 402 by sending a synchronization acknowledgement 404 to the user network firewall 110. The synchronization acknowledgement 404 helps the user network firewall 110 to ascertain that the TCP synchronization command 402 has been received and approved by the SP network firewall 114 and the SP network firewall 114 is now ready to interact with the user network firewall 110. The user network firewall 110 in turn sends an acknowledgement 406 to the SP network firewall 114 to acknowledge the receipt of the synchronization acknowledgement 404. The acknowledgement 406 also affirms the SP network firewall 114 that the user network firewall 110 is also ready for the interaction.

[0070] The user network firewall 110 then sends a registration request 408 to the SP network firewall 114, for example, in the form of the registration command 314. The SP network firewall 114 may thereupon send a registration reply 410 to the UNI module 116. The registration reply 410 indicates whether the registration request 408 has been accepted or rejected by the SP network firewall 114. The user network firewall 110 acknowledges the receipt of the registration reply 410 by sending the acknowledgement 406, to the SP network firewall 114, once again. Once registered, the user network firewall 110 may send the shared access rules to the SP network firewall 114 using for example, the data packet 300.

[0071] In one implementation, the user network firewall 110 regularly sends a keep-alive signal 412 to perform a keep-alive check for verifying whether the destination firewall is active and ready for filtering data. The keep-alive signal 412 may be sent, for example, at the keep-alive intervals 320 exchanged using the data packet 300 while sending the registration command 314. The SP network firewall 114 in turn sends a keep-alive reply 414 to indicate to the user network firewall 110 that the SP network firewall 114 is active and ready for filtering data. In case the SP network firewall 114 does not send the keep-alive reply 414, the user network firewall 110 assumes that the SP network firewall 114 is inactive. The user network firewall 110 in such a case starts filtering the data based on the shared access rules also. Additionally, the user

network firewall 110 may resend the TCP synchronization command 402 to the SP network firewall 114 to get an update when the SP network firewall 114 gets activated again. On being reactivated, the SP network firewall may reset the connection using the synchronization acknowledgement 404.

[0072] Further, whenever the user network firewall 110 needs to send the shared access rules to the SP network firewall 114 or update the already sent shared access rules, the user network firewall 110 sends an update request 416 to the SP network firewall 114. For example, the user network firewall 114 sends the update request 416 using the update command 324 for updating the access rules data 242 corresponding to the user network 104. In one implementation, the update request 416 may include all or few of the shared access rules that the user network 104 needs the SP network firewall 114 to apply for the user network firewall 114. The SP network firewall 114 then sends an update request reply 418 to acknowledge the receipt of the update request 416. In one implementation, the user network firewall 110 may skip the next scheduled keep-alive check as the update request reply 418 ensures that the SP network firewall 114 is active and is accepting the shared access rules. The user network firewall 110 may then regularly perform the keep-alive check with the SP network firewall.

[0073] Figure 5 illustrates exemplary method 500 for distributing shared access rules by a user network firewall, while Figure 6 illustrates methods 600 for configuring a service provider network firewall to implement access control based on the shared access rules, according to an embodiment of the present subject matter. Although the methods 500 and 600 as described in Figure 5 and Figure 6 are described for distributing access control using the DACP, it will be understood that access control may be distributed using other transmission mechanisms without deviating from the scope of the present subject matter.

[0074] The order in which the methods 500 and 600 are described is not intended to be construed as a limitation, and any number of the described method blocks can be combined in any order to implement the methods, or alternative methods. Additionally, individual blocks may be deleted from the methods without departing from the spirit and scope of the subject matter described herein. Furthermore, the methods can be implemented in any suitable hardware, software, firmware, or combination thereof.

[0075] A person skilled in the art will readily recognize that steps of the methods 500 and 600 can be performed by programmed computers. Herein, some embodiments are also intended to cover program storage devices, for example, digital data storage media, which are machine or computer readable and encode machine-executable or computer-executable programs of instructions, wherein said instructions perform some or all of the steps of the described methods. The program storage devices may be, for example, digital memories, magnetic storage media, such as a magnetic disks and magnetic tapes, hard drives, or optically readable digital data storage media. The embodiments are also intended to cover both communication network and communication devices configured to perform said steps of the exemplary methods.

[0076] Referring to Figure 5 illustrating the method 500, at block 502, access rules are identified for filtering data entering a user network, such as the user network 104. A user network firewall, for example, the user network firewall 110 of the user network 104 identifies one or more access rules from a plurality of access rules. As described previously, the identified access rules may be shared access rules that are shared with a service provider network, for example, the SP network 106 for filtering data entering or leaving the user network 104. Further, one or more access rules from the access rules may also be identified and implemented at the user network firewall 110. In one implementation, the UNARC module 218 of the user network firewall 110 identifies the access rules.

[0077] At block 504, a registration request for providing the access rules is sent to a service provider network firewall, for example, the SP network firewall 114. For example, the user network firewall 110 may send the registration request 408 seeking permission for transferring the access rules to the SP network firewall 114. In one implementation, the user network firewall 110 may use a distributed access control protocol to send the registration request 408, for example, along with the registration command 314. In one embodiment, registration process may be performed before identification of the access rules as defined at the block 502. For example, a registration request may be sent initially as soon as the user network firewall 110 boots up. The user network firewall 110 can register with SP network firewall 114 and maintain an open connection which can be used to share information, such as the shared access rules whenever required.

[0078] At block 506, a determination is made to ascertain whether the registration request 408 has been accepted by the SP network firewall 114. For example, the user network firewall 110 checks the registration reply 410 to determine whether the SP network firewall 114 has accepted the registration request 408. If the user network firewall 110 determines that the registration request 408 is denied, which is the 'No' path from the block 506, it implements the access rules at the user network firewall 110 at block 508. In one implementation, the user network firewall 110 applies the access rules to block unauthorized data entering or leaving the user network 104. It will be appreciated that upon the registration request 408 being denied, the shared access rules as well as the unshared access rules are implemented at the user network firewall 110.

[0079] In case it is determined that the registration request is accepted by the SP network firewall 114, which is the 'Yes' path from the block 506, the access rules, such as the shared access rules, are provided to the SP network firewall at the block 510. For example, the user network firewall 110 may send the access rules using a distributed access control protocol in the form of the data packet 300. In another implementation, the access rules may be provided using other transmission mediums such as emails or portable storage device. Further, the user network firewall 110 may also encrypt the access rules before sending the access rules to the SP network firewall 114. Also, the shared access rules may be implemented at the user network firewall 110 until an acknowledgement is received from the SP network firewall 114. Implementing the shared access rules at the user network firewall 110 ensures network safety in case there is some delay between transfer of the shared access rules by the user network firewall 110 and its receipt and acknowledgement by the SP network firewall 114. Thus, access rules can be provided to a service provider network firewall for filtering unauthorized data from data entering or leaving a user network subscribed with the service provider network.

[0080] Referring to Figure 6 illustrating the method 600, at block 602, a user network firewall is registered, with a service provider network firewall. For example, the SP network firewall 114 may register the user network firewall 110 on receiving a registration request 408 from the user network firewall 110. For the purpose, the SP network firewall 114 may first check user network account details to verify whether the user network 104 has paid a service fees. Additionally the SP network firewall 114 may also check the current load handled by the SP network firewall 114 to ascertain if it can handle the services requested by the user network

firewall 110. The SP network firewall 110 may then authenticate the user network (104) based on the verification. Additionally, the SP network firewall 114 may also use the authentication keys, such as a hash value to register the user network firewall 110.

[0081] At block 604, access rules, for example the shared access rules, are received from the user network firewall 110. The access rules may be received from the user network firewall 110 by the SP network firewall 114, on successful authentication of the user network firewall 110 by the SP network firewall 114. In one implementation, the access rules may be received using a transmission protocol, for example, the DACP in the form of data packets. The data packets may be received by the SP interaction module 118 of the SP network firewall 114. In one implementation, the data packets received by the SP interaction module 118 may be encrypted such that the SP interaction module 118 decrypts the data packets to obtain the access rules. In another implementation, the access rules may be received using other transmission mediums such as emails or portable storage device.

[0082] At block 606, access rules data corresponding to the user network firewall 110 is updated based on the access rules received from the user network firewall 110. For example, the SP network firewall 114 receives the access rules from user network firewall 110 and adds them to the already existing access rules saved in the access rules data 242 corresponding to the user network firewall 110. Further, the SP network firewall 114 may also create a new set of access rules data 242 based on the access rules received from the user network firewall 110.

[0083] At block 608, the access rules are implemented for a user network corresponding to the user network firewall 110 sending the access rules. For example, the SP network firewall 114 applies the access rules to regulate data traffic entering or leaving the user network 104. In one implementation, the access rules are provided to an access control module, for example, the SP access control module 244 of the SP network firewall 114 for filtering unauthorized data from the data packets directed towards the user network 104. The SP access control module 244 then analyzes the data packets and identifies the unauthorized data based on the access rules and blocks the unauthorized data entering the user network 104.

[0084] Thus a service provider network firewall can be configured to implement access control rules for filtering data entering or leaving a user network firewall subscribed with the service provider network firewall. Implementing the access rules at the service provider network

firewall helps in improving bandwidth utilization of the user network firewall. It further helps the service provider in improving its services by providing extra services to the user network at same or some additional charges. Additionally, implementing the access rules at the service provider network firewall ensures improved safety for the user network as the service provider network firewall is usually technically advanced and configured to handle more load in lesser time as compared to the user network firewall.

[0085] Although implementations for distributing access control across network firewalls have been described in language specific to structural features and/or methods, it is to be understood that the appended claims are not necessarily limited to the specific features or methods described. Rather, the specific features and methods are disclosed as exemplary implementations for access control distribution.

CLAIMS

1. A method comprising:
 - identifying, at a user network (104), at least one access rule, wherein the access rule is implementable at a service provider network firewall (114) for filtering data directed to the user network (104); and
 - providing the at least one access rule to the service provider network firewall (114) for implementing the at least one access rule at a service provider network (106).
2. The method as claimed in claim 1, further comprises registering the user network (104) with the service provider network firewall (114).
3. The method as claimed in claim 1, wherein the providing the at least one access rule comprises transmitting an authentication key to the service provider network firewall (114).
4. The method as claimed in claim 3, wherein the authentication key is a hash value, and wherein the hash value is generated using pre-existing parameters available with the user network (104) and the service provider network (106).
5. The method as claimed in claim 1, wherein the providing the at least one access rule comprises encrypting the at least one access rule.
6. The method as claimed in claim 1, wherein the providing the at least one access rule comprises transmitting the at least one access rule using a distributed access control protocol.
7. The method as claimed in claim 1, wherein the identifying further comprises ascertaining one or more access rules implementable at a user network firewall (110).
8. A method comprising:
 - receiving at least one access rule from a user network firewall (110); and
 - implementing the at least one access rule at a service provider network firewall (114) for filtering data directed to a user network (104).
9. The method as claimed in claim 8, further comprises:
 - receiving a registration request from the user network firewall (110); and
 - registering the user network firewall (110) to permit transmission of the at least one access rule.
10. The method as claimed in claim 9, wherein the registering comprises:

- analyzing user network account details to verify payment of service fees by the user network (104);
- authenticating the user network (104) based on the analysis.
11. The method as claimed in claim 8, wherein the receiving the at least one access rule comprises:
- receiving, using a distributed access control protocol, at least one encrypted data packet having the at least one access rule and
- decrypting the encrypted data packets to obtain the at least one access rule.
12. A user network access control (UNAC) system (108) comprising:
- a processor (202); and
- a memory (206) coupled to the processor (202), the memory (206) comprising:
- a user network access rule configuration (UNARC) module (218) configured to identify at least one access rule implementable at a service provider network firewall (114) for filtering data intended for a user network (104); and
- a user network interaction module (116) configured to provide the at least one access rule to the service provider network firewall (114).
13. The UNAC system (108) as claimed in claim 12, wherein the user network interaction module (116) is configured to provide the at least one access rule based on a distributed access control protocol.
14. The UNAC system (108) as claimed in claim 12, wherein the UNARC module (218) is further configured to:
- receive a plurality of access rules; and
- analyze the plurality of access rules to identify at least one access rule implementable at the service provider network firewall (114) and one or more access rules implementable at the user network firewall (110).
15. The UNAC system (108) as claimed in claim 12, wherein the at least one access rule includes at least one of Internet protocol address based rules, content based rules, and application based rules.
16. A service provider access control (SPAC) system (112) comprising:
- a processor (208); and
- a memory (212) coupled to the processor (208), the memory (212) comprising:

a service provider interaction module (118) configured to receive at least one access rule; and

a service provider network access control module (244) configured to filter unauthorized data from data directed to a user network (104) based on the at least one access rule.

17. The SPAC system (112) as claimed in claim 16, wherein the service provider interaction module (118) is further configured to update access rules data corresponding to the user network (104) based on the at least one access rule.
18. A computer-readable medium having embodied thereon a computer program for executing a method comprising:
 - identifying, at a user network (104), at least one access rule implementable at a service provider network firewall (114) for filtering data directed to the user network (104); and
 - providing the at least one access rule to the service provider network firewall (114) for implementing the at least one access rule at a service provider network (106).
19. The computer readable medium as claimed in claim 18, wherein the providing the at least one access rule comprises transmitting, by a user network firewall (110), the at least one access rule using a distributed access control protocol.
20. A computer-readable medium having embodied thereon a computer program for executing a method comprising:
 - receiving at least one access rule from a user network firewall (110); and
 - implementing the at least one access rule at a service provider network firewall (114) for filtering data directed to a user network (104).

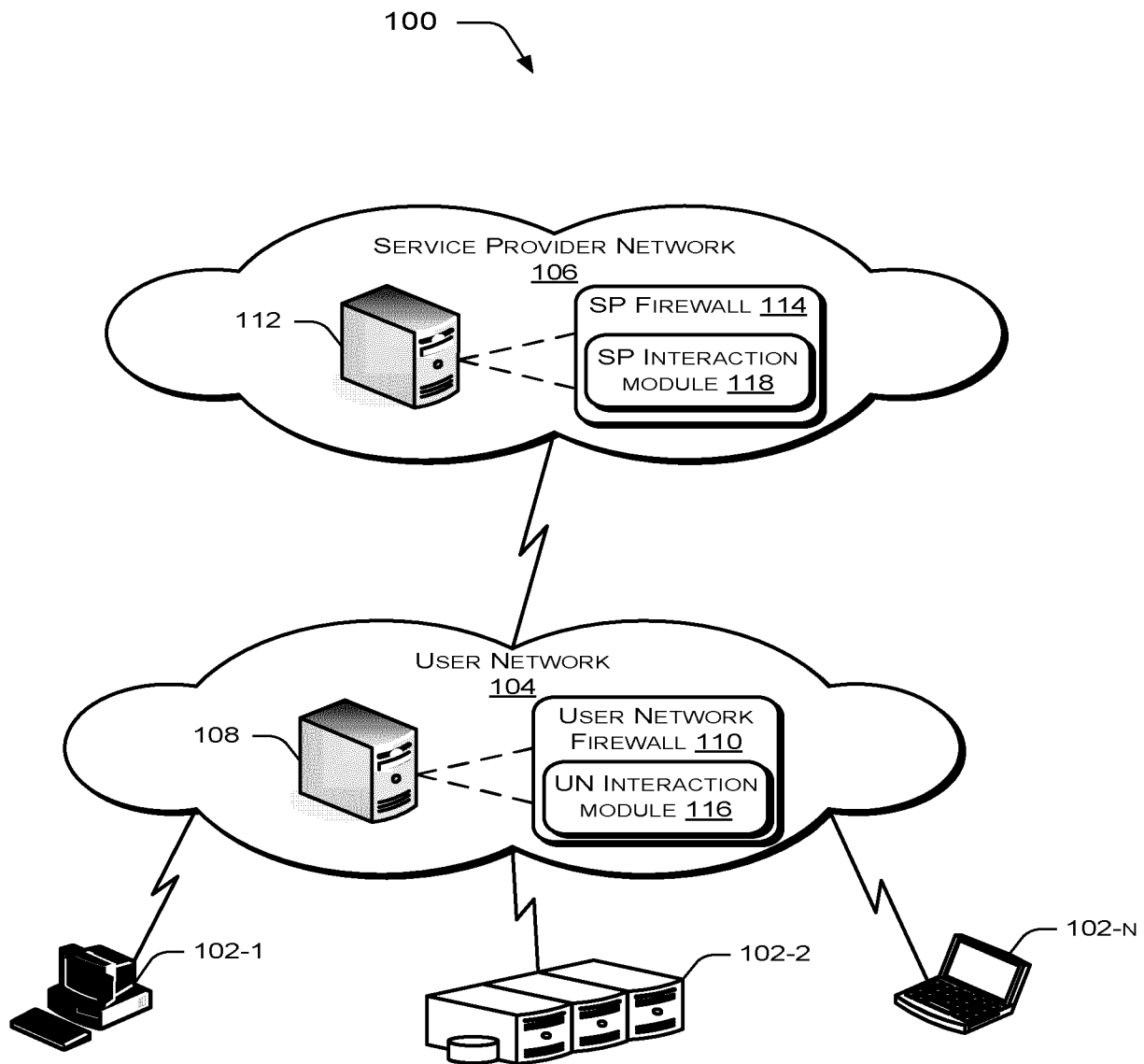


Fig. 1

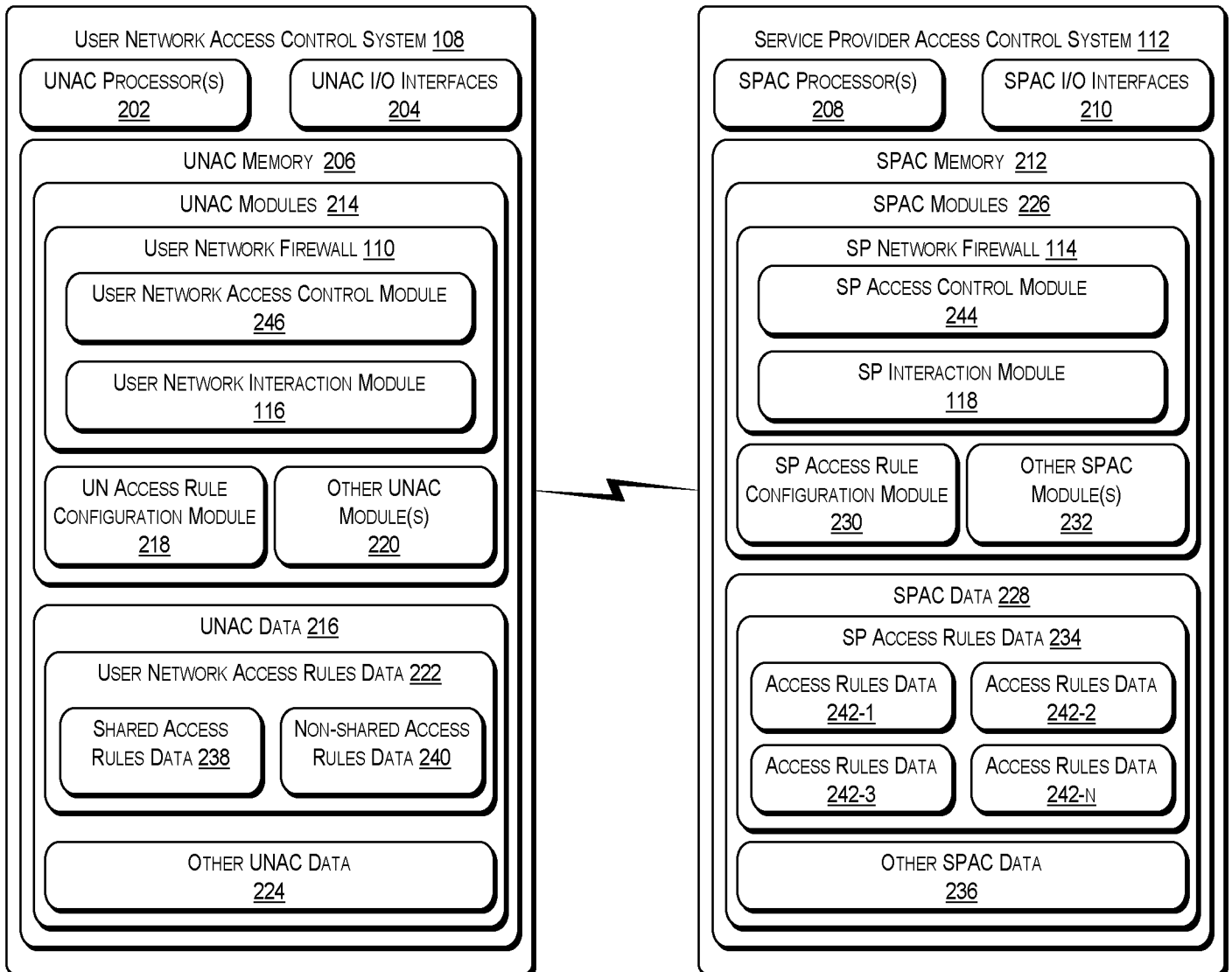


Fig. 2

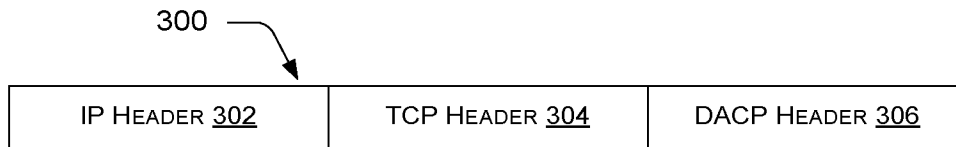


Fig. 3a



Fig. 3b

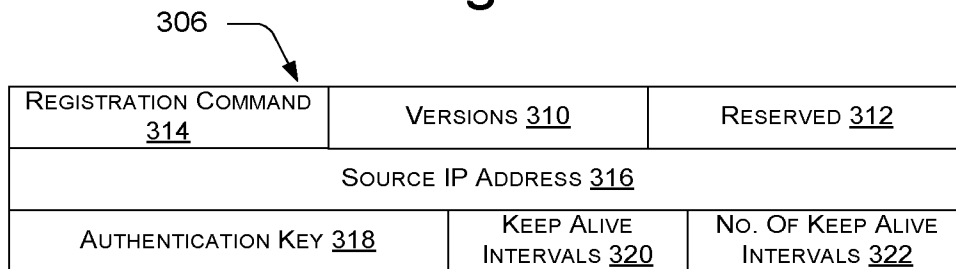


Fig. 3c

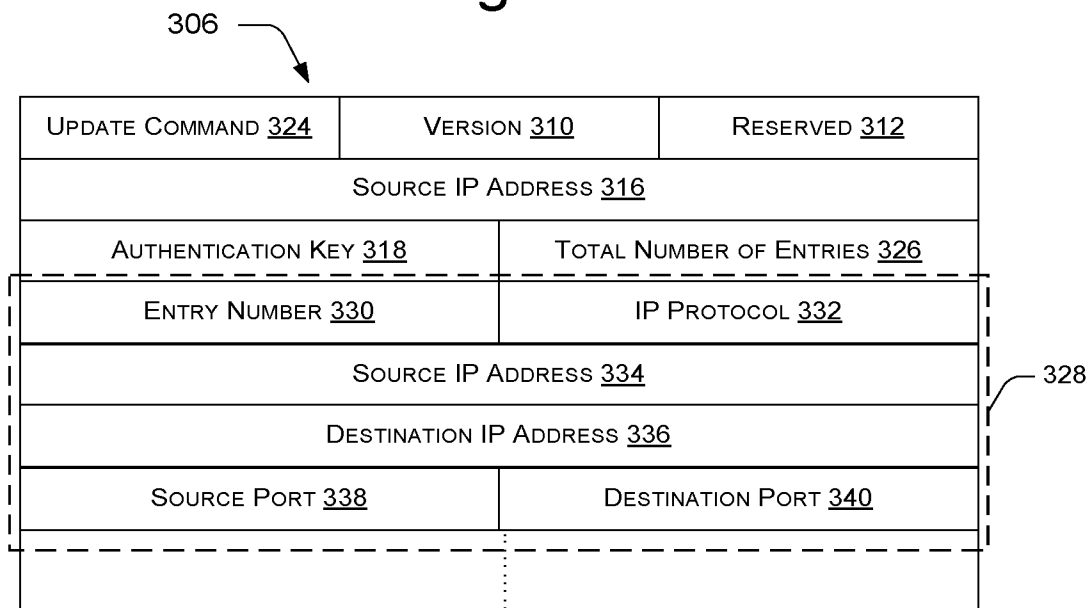


Fig. 3d

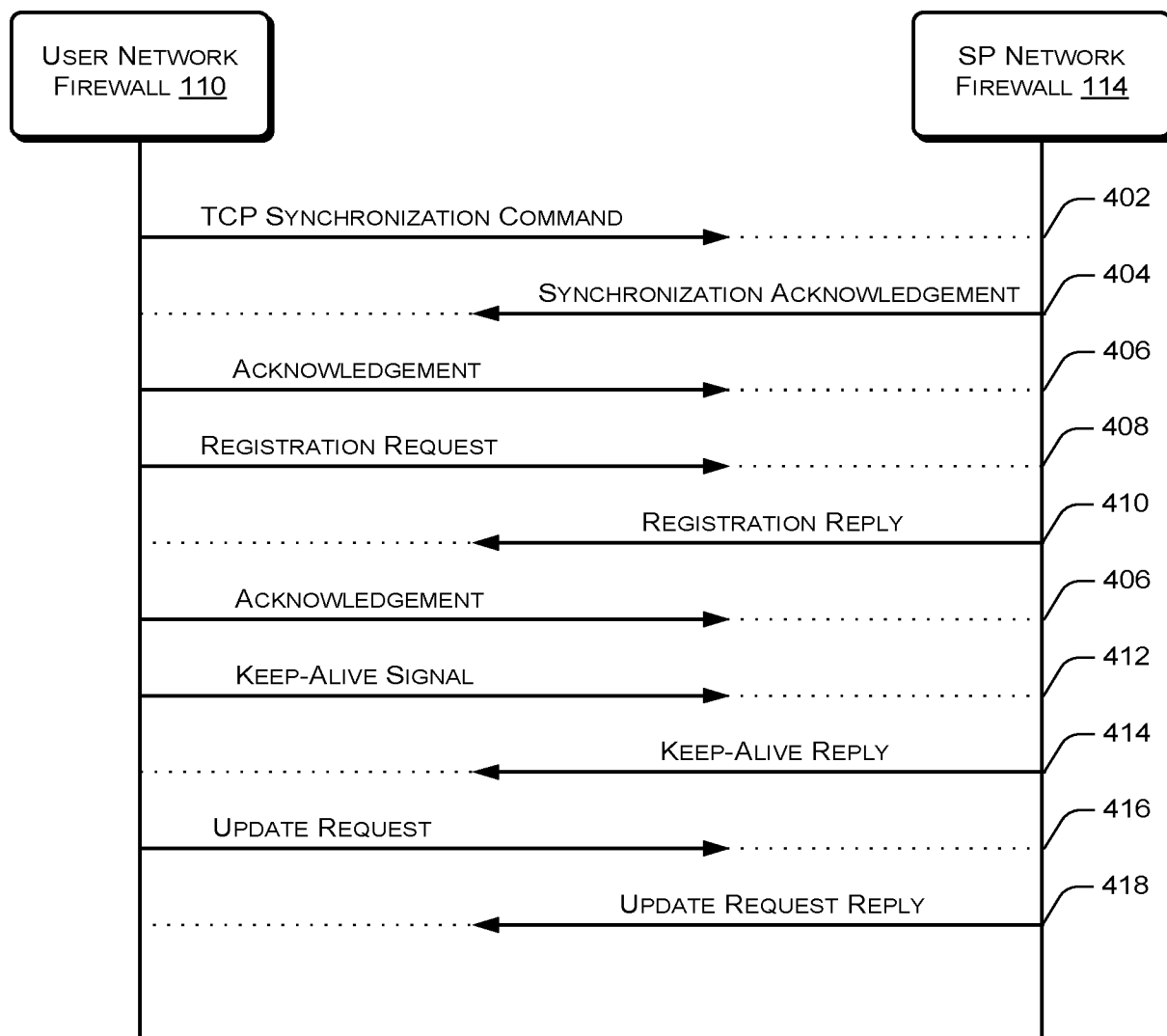
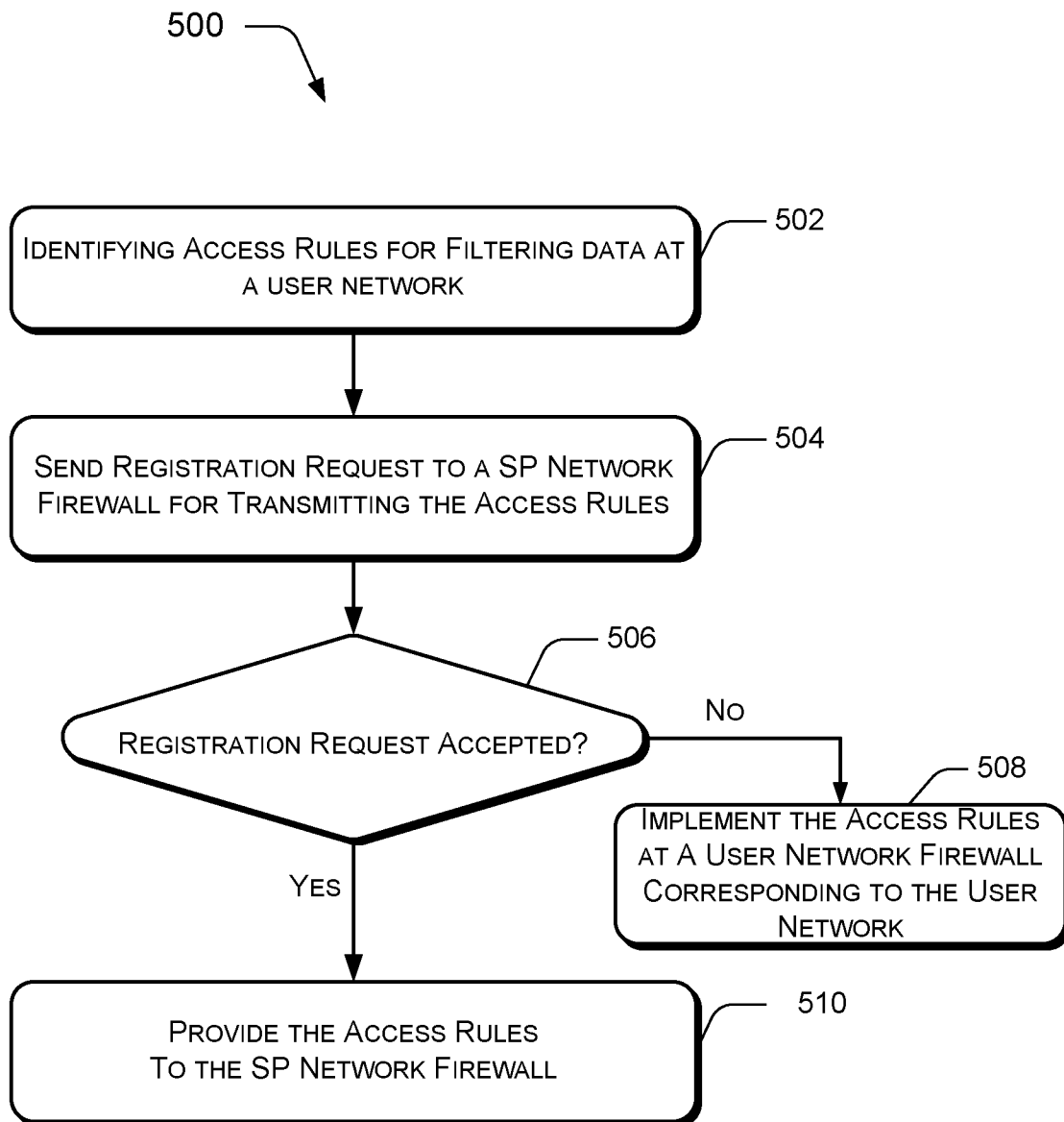


Fig. 4

**Fig. 5**

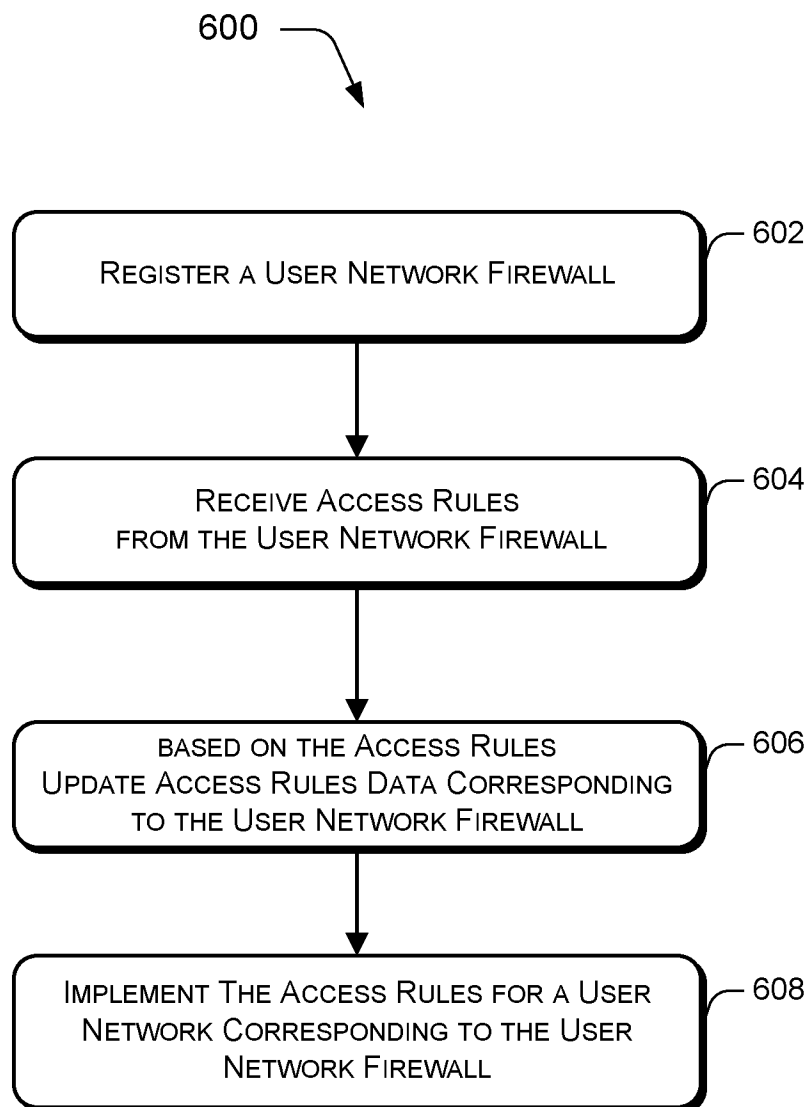


Fig. 6

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2012/056977

A. CLASSIFICATION OF SUBJECT MATTER
 INV. H04L29/06
 ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7 054 930 B1 (CHERITON DAVID [US]) 30 May 2006 (2006-05-30) abstract; claim 1; figures 1,6,7 column 3, lines 29-46 column 4, line 64 - column 6, line 3 column 8, line 54 - column 9, line 22 -----	1-20
X	WO 01/65343 A1 (CHECK POINT SOFTWARE TECHNOLOG [IL]; FRIEDMAN MARK M [IL]; FINK GONEN) 7 September 2001 (2001-09-07) abstract; figures 1,2,3 page 7, lines 15-28 page 8, line 13 - page 10, line 12 page 11, line 22 - page 13, line 28 ----- -/-	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

29 May 2012

Date of mailing of the international search report

06/06/2012

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Authorized officer

Schossmaier, Klaus

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2012/056977

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SMITH R N ET AL: "Operating firewalls outside the LAN perimeter", PERFORMANCE, COMPUTING AND COMMUNICATIONS CONFERENCE, 1999 IEEE INTERNATIONAL SCOTTSDALE, AZ, USA 10-12 FEB. 1999, PISCATAWAY, NJ, USA, IEEE, US, 10 February 1999 (1999-02-10), pages 493-498, XP010323674, ISBN: 978-0-7803-5258-2 abstract; figure 1 section 1 section 3	1-20
A	----- BUTLER K ET AL: "A Survey of BGP Security Issues and Solutions", PROCEEDINGS OF THE IEEE, IEEE. NEW YORK, US, vol. 98, no. 1, 1 January 2010 (2010-01-01), pages 100-122, XP011298700, ISSN: 0018-9219 abstract; table 2 section II.B sections III.B, III.E sections IV.A, IV.C -----	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2012/056977

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
US 7054930	B1	30-05-2006	US	7054930 B1		30-05-2006
			US	7779126 B1		17-08-2010

WO 0165343	A1	07-09-2001	AT	312463 T		15-12-2005
			AU	4171701 A		12-09-2001
			AU	2001241717 B2		22-12-2005
			BR	0109035 A		03-06-2003
			CA	2401577 A1		07-09-2001
			CN	1406351 A		26-03-2003
			DE	60115615 T2		06-07-2006
			EP	1266277 A1		18-12-2002
			HU	0300039 A2		28-05-2003
			IL	151522 A		03-12-2007
			JP	3954385 B2		08-08-2007
			JP	2003525557 A		26-08-2003
			NO	20024113 A		01-11-2002
			NZ	520984 A		28-02-2003
			PL	357181 A1		26-07-2004
			US	6496935 B1		17-12-2002
			WO	0165343 A1		07-09-2001
